Date: July 3, 2018

Version: 1.0

Revision	Date	Changes
1.0	July 3, 2018	Initial Release

Arista CloudVision Portal Incorrect Permissions Vulnerability - CVE-2018-12357

CVSS v3: 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

This advisory is to document a security vulnerability identified by Arista Networks that affects CloudVision Portal. Affected CloudVision Portal releases are listed in Table-1 below. This issue is an incorrect permissions vulnerability in which an authenticated user could gain access to sensitive information of other users. A prerequisite to this is the configuration of a remote AAA server.

NOTE:

This vulnerability was identified internally by Arista Networks and there have been no external reports of an exploit, as of the date of this notice.

Affected Software Releases:

2018	2017	2016	2015
2018.1 • 2018.1.0 • 2018.1.1	2017.2 • 2017.2.0 • 2017.2.1 • 2017.2.2 • 2017.2.3 2017.1 • 2017.1.0 • 2017.1.0.1 • 2017.1.1 • 2017.1.1.1	2016.1 • 2016.1.0 • 2016.1.1 • 2016.1.2 • 2016.1.2.1 • 2016.1.2.3	2015.1 • 2015.1.1 • 2015.1.2

Recommended Action:

For systems running any affected release of CloudVision Portal, the immediate recommendation is to:

- Follow the recommended mitigation to minimize risk
- Upgrade to a remediated version of CloudVision Portal for resolution

Mitigation:

Only authenticated users to CloudVision portal that have read or write access to ‘Account Management’ can exploit this vulnerability. The general recommendation is to restrict users assigned to the default ‘network-admin’ role to a trusted subset and for all other roles defined, remove read or write access to ‘Account Management’ using the following steps:

1. Click on Settings
2. In the Account Management tab, chose ‘Roles’ from the drop down menu
3. Ensure that the network-admin/network-operator role only includes a trusted subset of users
    - View the list of users assigned to the network-admin/network-operator role
    - Create a new role that does not have read or write access to User management
4. Review the rest of the role settings and users assigned to each role. In general, users should be restricted to a role that limits read and write access to only the modules they need. In particular, read and write access to the settings modules should be limited to CloudVision Portal administrators.

Resolution:

This vulnerability is tracked by bug 273526 and is addressed in CloudVision Portal release 2018.1.2. It is recommended to upgrade to the remediated version.

For More Information:

If you require further assistance, or if you have any further questions regarding this security notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

Open a Service Request:

By email: support@arista.com
By telephone: 408-547-5502
866-476-0000